(12) UK Patent Application (19) GB (11) 2 155 669 A

(43) Application published 25 Sep 1985

(21) Application No 8405854

(22) Date of filing 6 Mar 1984

(51) INT CL⁴
G06F 7/52

(52) Domestic classification
G4A 2BX MD
U1S 2106 2107 G4A

(56) Documents cited
GB A 2109135

(58) Field of search
G4A

(71) Applicant
Sony Corporation (Japan),
7–35 Kitashinagawa-6, Shinagawa-ku, Tokyo, Japan

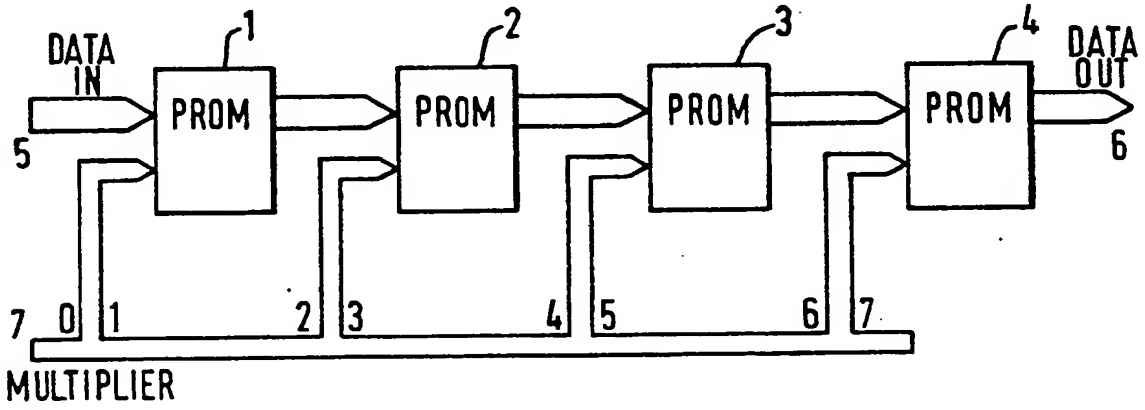
(72) Inventor
Clive Henry Gillard

(74) Agent and/or Address for Service
D Young & Co,
10 Staple Inn, London WC1V 7RD

(54) Galois field multipliers

(57) A Galois field multiplier for multiplying an arbitrary element β of a Galois field by α^n where α is another element of the Galois field and n is an integer, comprises a data path comprising an input (5) to which an input binary data word representing the element β is supplied, a plurality of programmable read-only memories (1, 2, 3, 4) connected in series in the path and each able to effect Galois field multiplication, an output (6) connected to the output of the final memory (4) and from which the Galois field multiplied data word is derived, and a control input (7) to which a multiplier data word representing n and consisting of a plurality of binary digits is supplied, one or more of the binary digits being supplied to each memory to control the multiplication effected by that memory.

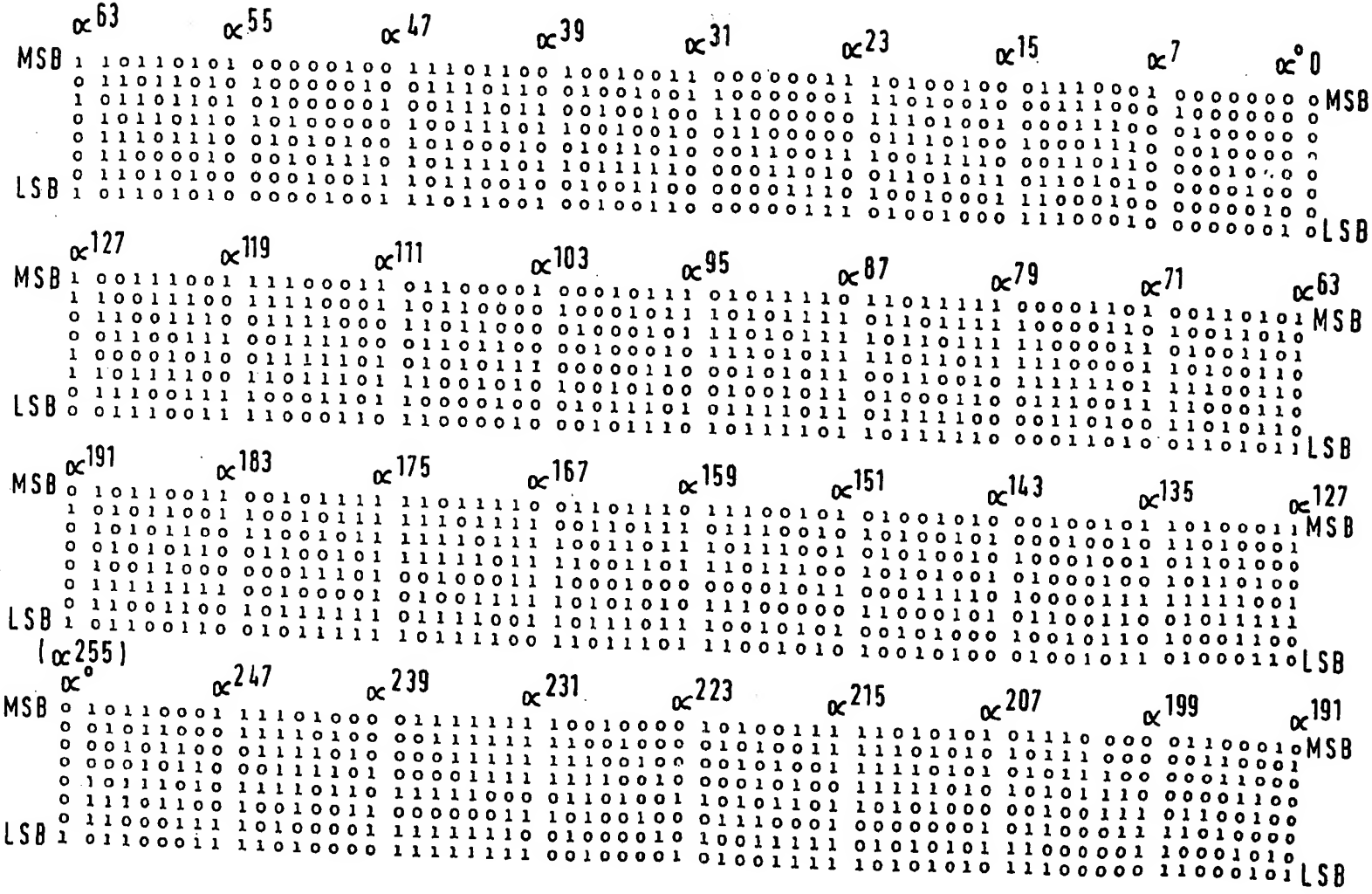
FIG. 3.



GB 2155669 A

The drawing(s) originally filed was/were informal and the print here reproduced is taken from a later filed formal copy.

FIG. 1.



2155669

FIG. 2.

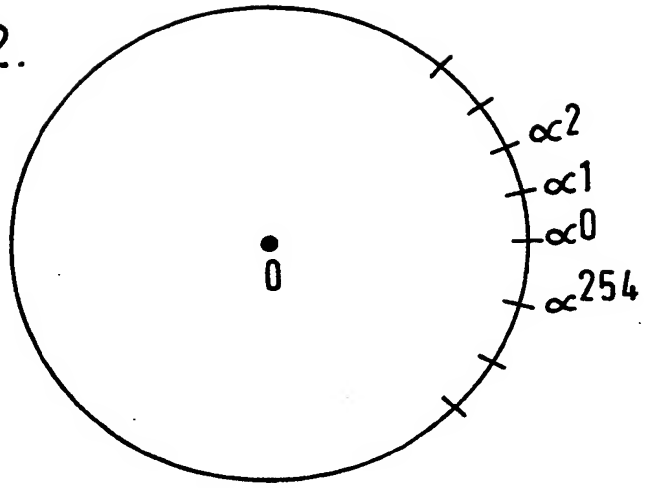
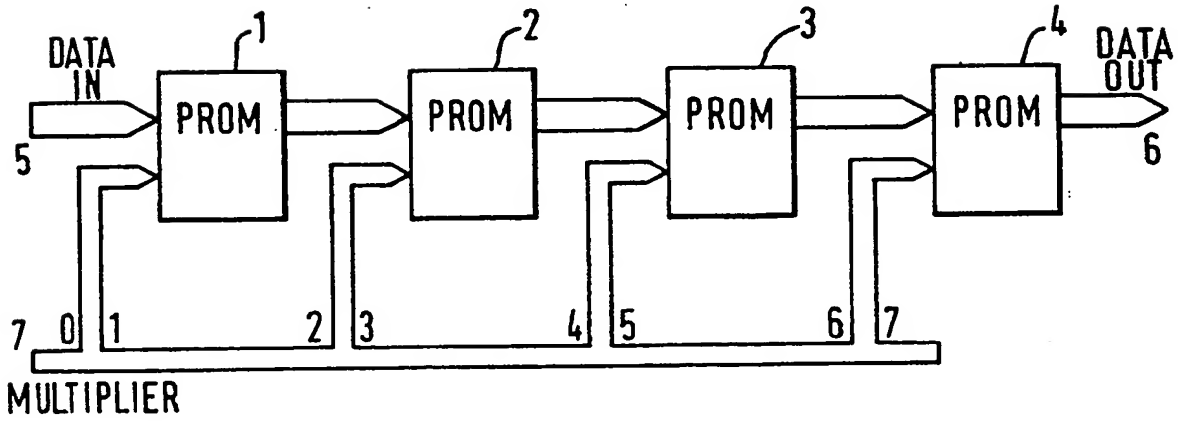

α2
α1
α0
α254
0

FIG. 3.


DATA IN
PROM
PROM
PROM
PROM
DATA OUT
1
2
3
4
5
6
7 0 1 2 3 4 5 6 7
MULTIPLIER

SPECIFICATION

Galois field multipliers

This invention relates to Galois field multipliers.

Where an error correcting code is used in binary data processing, for example to provide error correction where digital television signals are to be recorded and reproduced using a digital video tape recorder, Galois field arithmetic is commonly used as in some ways it is easier to implement than ordinary arithmetic, because there are no carries. A particular form of code which can use Galois field arithmetic and has been used in such cases is the Reed Solomon code, which may be produced by a generator polynomial using a function of the extension field of a primitive polynomial, for example, as represented by $GF(2^8)$:

$$X^8 + X^4 + X^3 + X^2 + X^0 = 0 \qquad (1)$$

The primitive element α and other elements are generated using:

$$\alpha^8 = \alpha^4 + \alpha^3 + \alpha^2 + 1 \qquad (2)$$

The H-matrix for this primitive polynomial is shown in Fig. 1 of the accompanying drawings, where MSB and LSB refer to the most and least significant bits, respectively.

Another way of considering the process of Galois field multiplication will now be described with reference to Fig. 2 of the accompanying drawings. The centre of the circle shown represents the 8-bit word 00000000. Around the circumference of the circle are 255 steps designated α^0, α^1, α^2, . . . α^{254} representing all the different non-zero patterns of an 8-bit code. A Galois field multiplier can be used to step an input data word around the circle. Thus, when an 8-bit data word is supplied to the Galois field multiplier, the input data word may be considered as having been multiplied by α^0, that is by 1. Each successive shift or multiplication by α^1 has the effect of moving the input data word by one step around the circle, up to a maximum of α^{254}. One further shift or multiplication will bring the input data word back to the original value. Because the polynomial is primitive, any input 8-bit combination other than 00000000 supplied to the Galois field multiplier will cycle in a predetermined manner through all the other possible combinations before returning to the original combination.

In decoding an error correcting code, therefore, each input data word can be stepped or multiplied by any desired power of α in a Galois field multiplier. One prior example of a Galois field multiplier is shown in Fig. 6.3 on page 162 of "Error Control Coding—Fundamentals and Applications" by Shu Lin and Daniel J. Costello, published in 1983. This prior Galois field multiplier comprises a feedback shift register, and pulsing of the shift register effects Galois field multiplication of an arbitrary element β in the Galois field by α. Successive shifts of the register will generate vector representations of successive powers of α, in accordance with particular functions of the Galois field of the generator polynomical used, which in this particular case is:

$$GF(2^4) = X^4 + X + 1 \qquad (2)$$

Likewise, Fig. 6.4 on the same page shows a Galois field multiplier for multiplying an arbitrary element β in $GF(2^4)$ by α^3.

In error correction circuits it is commonly necessary, as described above, to multiply β by α^n, where β and α^n are elements in a Galois field and n is a variable integer. Moreover, in such error correcting circuits the data rate may be such that the multiplications need to be carried out at a very high frequency; in one particular example one such multiplication was required every 74 nanoseconds. In such a case a Galois field multiplier comprising a shift register is too slow.

According to the present invention there is provided a Galois field multiplier for multiplying an arbitrary element β of a Galois field by α^n where α is another element of the Galois field and n is an integer, the Galois field multiplier comprising:

a data path comprising an input to which an input binary data word representing the element β to be Galois field multiplied is supplied;

a plurality of multiplier elements connected in series in said path and each able to effect Galois field multiplication, and an output connected to the output of the final said multiplier element and from which the Galois field multiplied data word is derived; and

a control input to which a multiplier data word representing n and consisting of a plurality of binary digits is supplied, one or more of said binary digits being supplied to each said multiplier element to control the multiplication effected by that multiplier element.

The invention will now be described by way of example with reference to the accompanying drawings, in which:

Figure 1 shows the H-matrix of the primitive polynomial of equation (1);

Figure 2 shows diagrammatically an operation of a Galois field multiplier; and

Figure 3 shows in block form an embodiment of Galois field multiplier according to the present invention.

Referring to Fig. 3, the embodiment of Galois field multiplier to be described comprises a series of multiplier elements, in the present case four programmable read-only memories (PROMs) 1, 2, 3 and 4. Input 8-bit data words representing arbitrary elements β of the Galois field and to which the Galois

field multiplication is to be applied are supplied successively to an input 5 connected to a data input of the PROM 1. Subsequent to the multiplication the multiplied data word is supplied by way of an output from the PROM 1 to an input of the PROM 2 and so on until the final multiplied output is supplied from an output of the PROM 4 to an output 6.

The number of multiplications, or in the terminology used above, the power n to which α is raised, is determined by an 8-bit multiplier word which is supplied by way of an input 7. Numbering the bits of the multiplier word from the least significant bit to the most significant bit as 0 to 7, the bits 0 and 1 are supplied to control the PROM 1, the bits 2 and 3 are supplied to control the PROM 2, the bits 4 and 5 are supplied to control the PROM 3, and the bits 6 and 7 are supplied to control the PROM 4. Thus, the PROM 1 can shift or multiply the input data word by α to the power 0, 1, 2 or 3. The PROM 2 can shift or multiply the multiplied input data word received from the PROM 1 by α to the power 0, 4, 8 or 12. The PROM 3 can shift or multiply the multiplied input data word received from the PROM 2 by α to the power 0, 16, 32 or 48. The PROM 4 can shift or multiply the multiplied input data word received from the PROM 3 by α to the power 0, 63, 128 or 192.

Thus, by suitable selection of the multiplier word supplied to the input 7 any desired number of shifts or multiplications up to a maximum of 255 can be achieved. For example, if 123 multiplications are required, then the multiplier word, reading from the most significant digit, would be 011110111, and the PROMs 1 to 4 would effect shifts of 3, 8, 48 and 64 respectively, giving the required total shift of 123, so the 8-bit data output supplied to the output 6 would represent $\beta\,\alpha^{123}$, which by definition is another element of the Galois field used.

In the particular embodiment described, the PROMs 1 to 4 can each be a 1K × 8 PROM.

Clearly many modifications are possible. For example, the particular choice of an 8-bit data word, an 8-bit multiplier, and the number of PROMs in the described embodiment are merely given by way of example. Advantages will be gained in reduced memory capacity in any case where the number of shifts or multiplications is divided between two or more PROMs.

If the circuit was arranged with eight series connected multiplier elements, so that each multiplier element was controlled by only one bit of the multiplier word n, then each of the multiplier elements could be a random logic circuit. In the case described above, the eight multiplier elements would then multiply by α to the power 0 or 1; α to the power 0 or 2; α to the power 0 or 4; α to the power 0 or 8; α to the power 0 or 16; α to the power 0 or 32; α to the power 0 or 64; and α to the power 0 or 128, respectively Such an arrangement is advantageous where a special integrated circuit incorporating all the multiplier elements is to be designed for effecting the Galois field multiplication.

CLAIMS

1. A Galois field multiplier for multiplying an arbitrary element β of a Galois field by α^n where α is another element of the Galois field and n is an integer, the Galois field multiplier comprising:
a data path comprising an input to which an input binary data word representing the element β :o be Galois field multiplied is supplied;
a plurality of multiplier elements connected in series in said path and each able to effect Galois field multiplication, and an output connected to the output of the final said multiplier element and from which the Galois field multiplied data word is derived; and
a control input to which a multiplier data word representing n and consisting of a plurality of binary digits is supplied, one or more of said binary digits being supplied to each said multiplier element to control the multiplication effected by that multiplier element.

2. A multiplier according to claim 1 wherein each said multiplier element is a programmable read-only memory.

3. A multiplier according to claim 2 comprising four said memories, and wherein said multiplier data word consists of eight binary digits, respective pairs of which are supplied to respective said memories.

4. A multiplier according to claim 1 wherein each said multiplier element is a logic circuit.

5. A multiplier according to claim 4 comprising eight said logic circuits, and wherein said multiplier data word consists of eight binary digits, respective digits of which are supplied to respective said logic circuits.

6. A Galois field multiplier substantially as hereinbefore described with reference to Fig. 3 of the accompanying drawings.

Printed in the United Kingdom for
Her Majesty's Stationery Office, Dd 8818935, 1985, 4235.
Published at The Patent Office, 25 Southampton Buildings, London, WC2A 1AY, from which copies may be obtained.